(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 July 2001 (12.07.2001)

PCT

(10) International Publication Number
WO 01/50299 A2

(51) International Patent Classification[7]: G06F 17/00

(21) International Application Number: PCT/IL00/00843

(22) International Filing Date:
17 December 2000 (17.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/474,265 29 December 1999 (29.12.1999) US
09/710,898 14 November 2000 (14.11.2000) US

(71) Applicant *(for all designated States except US)*: **PANGO SYSTEMS B.V.** [NL/NL]; Paasheuvelweg 50, NL-1105 BJ Amsterdam (NL).

(72) Inventors; and

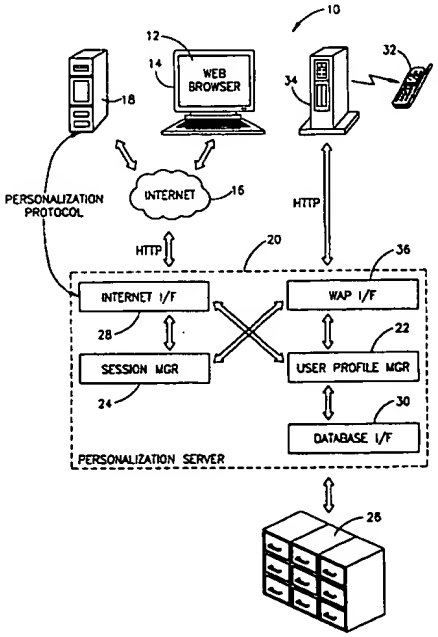
(75) Inventors/Applicants *(for US only)*: **LEVY, Ran** [IL/IL]; Palmah Street 8, 46793 Herzliya (IL). **SHAI, Avi** [IL/IL]; Yehoshua Tahon Street 10, 60920 Kadima (IL). **PALGI, Boaz** [IL/NL]; President Kennedylaan 166, NL-1079 NM Amsterdam (NL).

(74) Agent: **BRASS, Daniel**; Plinner, Bodner, Brass, Beit Agish Ravad, Noach Mozes Street 13, 67442 Tel Aviv (IL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DE (utility model), DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR INCREMENTAL DISCLOSURE OF PERSONAL INFORMATION TO CONTENT PROVIDERS



(57) Abstract: A method and a system for protecting the privacy of the user, while enabling the user to predetermine the disclosure of selected items of information to particular Web sites, for example according to the type of Web site and/or the type of information. Preferably, the user may optionally select a mode in which the permission of the user is requested each time that a particular type of information is requested by the Web site content provider. These items of information are preferably collected into a user profile, for which disclosure is controlled according to a disclosure policy. Also preferably, the user is able to control the overall disclosure of items of information by first selecting a browsing mode, such that the disclosure of a plurality of items of information is determined according to the browsing mode. According to preferred embodiments of the present invention, the distribution of cookies is also controlled according to the disclosure policy. Preferably, the

[Continued on next page]

WO 01/50299 A2

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

distribution is generally controlled according to whether the browsing mode is anonymous, such that the identify of the user is not provided; or involves the identification of the user. According to other preferred embodiments of the present invention, a content provider profile and a user profile is created for the content provider and the user, respectively. These two profiles can then optionally be compared in a process of negotiation, in order to determine if the user information should be disclosed to the content provider.

SYSTEM AND METHOD FOR INCREMENTAL DISCLOSURE OF PERSONAL INFORMATION TO CONTENT PROVIDERS

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a system and method for incremental disclosure of personal information to content providers, and in particular, to such a system and method in which the user is able to select which personal information is disclosed through the Internet, for example while viewing a Web page, as well as the circumstances under which that information is to be disclosed.

Web pages are popular for both Web page viewers, who may wish to receive information and/or to be entertained, and for Web page providers, who can reach a wide audience through the Internet. In order to tailor the content of the Web pages to the interests of the Web page viewers, and hence to attract more viewers and/or to attract viewers which fit a particular profile, Web page providers attempt to gather as much information as possible concerning the interests of the Web page viewers.

One mechanism for gathering such information is the provision of "cookies", which can be used to create a stateful session with HTTP (HyperText Transfer Protocol) requests and responses, as described in RFC 2109 (*RFC 2109: HTTP State Management Mechanism*, D. Kristol and L. Montulli, February 1997; *http://www.cis.ohio-state.edu/htbin/rfc/rfc2109.html* as of December 28, 1999). Cookies enable client Web browsers and Web servers to exchange state information across Web pages, for example in order to tailor content for individual Web page viewers, or to create "shopping carts" for online visitors to a Web site. The Web server of a content provider can initiate the creation of a cookie by sending state information to the client Web browser at any time. If the client Web browser accepts the cookie, the information is stored locally at the computer operating the client Web browser, and must be returned to the Web server with every subsequent request.

HTTP cookies enable Web page providers to create and manage private databases for storing information about Web page viewers who visit the Web pages of the provider. When the Web page viewer returns to the Web pages of the provider, the Web server requests the cookies from the Web browser of that viewer, and retrieves the information stored inside the cookies as a key to search through the private database for information about the Web page viewer. The Web page content which is to be displayed by that Web page viewer is then tailored according to the information stored in the database.

Another common mechanism for identifying Web page viewers uses regular HTML to store hidden keys which uniquely identify the viewer, such that the Web server generates Web pages containing these keys on the fly.

HTTP cookies and HTML with hidden keys have the advantage of being part of the standard for communication through the World Wide Web. Most widely available Web browsers, such as Netscape™ Navigator™ and Microsoft™ Internet Explorer™, support cookies. Indeed, cookies have become a common mechanism for tracking the behavior of Web page viewers, and for identifying return visitors to a Web site, thereby enabling the content provider to tailor the content of the Web site to the personal preferences of the viewers. On the other hand, the identification of such personal preferences, and the storage of the associated information in a remote database over which the Web page viewer has no control, raises a number of privacy-related issues.

First, personal information which identifies the Web page viewer, such as the name, home address and credit card number, may be stored in such databases, thereby threatening end-user privacy. Such identifying information is not necessary to identify a return visitor to a Web site for the purpose of tailoring content for that user. Furthermore, the fact that such information is stored may cause Web page viewers to feel uncomfortable with the entire process of gathering information, such that the viewers may wish to limit any information which is gathered, for example by rejecting all cookies, or by providing only limited personal information to the content provider. This in turn may result in the provision of Web page content which is less tailored to the needs of the viewer, and hence to a less satisfying Web page experience.

On the other hand, many viewers are not aware of the ability to accept or reject cookies by their Web browser, or of the privacy implications of such cookies. Indeed, the default behavior of most Web browsers is to accept all requests for cookies. Therefore, these Web page viewers may experience implicit unauthorized infringement of their privacy.

These local, private databases are also disadvantageous for the content provider, since the collected user information is based solely on the experience of the Web page viewer within the Web site of that particular content provider, thereby reflecting only part of the personality and interests of the user. Furthermore, the content provider may overestimate the importance of such information to the Web page viewer, even if the Web browsing experience from which the information was gathered represents only a transient phase of the life of the Web page viewer.

A more preferred solution would enable the content provider to also receive a personal profile of the Web page viewer, containing user information about a plurality of characteristics

of the user. The content provider could then integrate this profile-derived information with information derived from observing the actions of the Web page viewer when browsing through the Web site of the content provider, for a more complete picture of the interests of the user. Currently, users might be wary of providing such personal information, as previously described. However, the preferred solution would also include privacy protection, such that the user could determine when and how the information is released. Such a solution would thus combine privacy protection with more accurate information gathering, thereby benefiting both the Web page viewer and the content provider. Unfortunately, such a solution does not currently exist.

There is thus a need for, and it would be useful to have, a system and a method for both providing a personal profile to a content provider when a user is operating a Web browser, and for enabling the user to select when and how the information contained in the personal profile is released to the content provider.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, wherein:

FIG. 1 is a flowchart of an exemplary method for determining a personal profile and disclosure policy according to the present invention; and

FIGS. 2A and 2B are flowcharts of exemplary methods according to the present invention for handling HTTP cookies;

FIG. 3 is a schematic block diagram of an exemplary system according to the present invention;

FIG. 4 is a flowchart of an exemplary method according to the present invention for creation and matching of profiles for users and content providers; and

FIG. 5 is a schematic block diagram of a second exemplary but preferred embodiment of the system of the present invention.

SUMMARY OF THE INVENTION

The present invention is of a method and a system for protecting the privacy of the user, while enabling the user to predetermine the disclosure of selected items of information to particular Web sites, for example according to the type of Web site and/or the type of information. Preferably, the user may optionally select a mode in which the permission of the

user is requested each time that a particular type of information is requested by the Web site content provider. These items of information are preferably collected into a user profile, for which disclosure is controlled according to a disclosure policy. Also preferably, the user is able to control the overall disclosure of items of information by first selecting a browsing mode, such that the disclosure of a plurality of items of information is determined according to the browsing mode. Alternatively, the browsing mode may optionally be determined automatically or by the content provider.

According to preferred embodiments of the present invention, the distribution of cookies is also controlled according to the disclosure policy. Preferably, the distribution is generally controlled according to whether the browsing mode is anonymous, such that the identity of the user is not provided; or involves the identification of the user.

According to the present invention, there is provided a method for controlling disclosure of a plurality of items of information to a content provider by a user, the method comprising the steps of: (a) associating each item of information with a type of disclosure, such that the disclosure of the item of information to the content provider is determined according to the type of disclosure; (b) examining the type of disclosure to determine if disclosure of the item of information to the content provider is permitted; and (c) if disclosure is permitted, disclosing the item of information to the content provider.

According to another embodiment of the present invention, there is provided a system for controlling disclosure of a plurality of items of information by a user, the system comprising: (a) a Web site content provider for requesting an item of information from the user in a request; (b) a proxy server for intercepting the request; (c) a user personal profile for containing the plurality of items of information, including at least one type of disclosure for determining whether the item of information is disclosed to the Web site content provider by the proxy server.

According to yet another embodiment of the present invention, there is provided a method for controlling disclosure of a plurality of items of information to a content provider by a user, the content provider having an associated Web site, the method comprising the steps of: (a) associating each item of information with a type of disclosure, such that the disclosure of the item of information to the content provider is determined according to the type of disclosure; (b) accessing the Web site by the user; (c) requesting disclosure of an item of information by the content provider; (d) automatically examining the type of disclosure to determine if disclosure of the item of information to the content provider is permitted; and (e) if disclosure is permitted,

disclosing the item of information to the content provider. According to an alternative embodiment, steps (b) and (c) are reversed in the order of execution.

According to still another embodiment of the present invention, there is provided a method for controlling disclosure of a plurality of items of information to a content provider by a user, the method comprising the steps of: (a) receiving the plurality of items of information from the user; (b) associating each item of information with a type of disclosure according to a request of the user, such that the disclosure of the item of information to the content provider is determined according to the type of disclosure; (c) storing the plurality of items of information in a database; and (d) accessing the database by the user to alter an item in the database.

Hereinafter, the term "computer" includes, but is not limited to, personal computers (PC) having an operating system such as DOS, Windows™, OS/2™ or Linux; Macintosh™ computers; computers having JAVA™-OS as the operating system; and graphical workstations such as the computers of Sun Microsystems™ and Silicon Graphics™, and other computers having some version of the UNIX operating system such as AIX™ or SOLARIS™ of Sun Microsystems™; the Palm OS; embedded operating systems for mobile telephones, as well as WAP-enabled devices and other cellular telephone devices which are able to receive content through the Internet, or any cellular telephone device which communicates according to the I-mode protocol (Japanese packet-based cellular telephone communication protocol) or UMTS (Universal Mobile Telecommunications System; also a mobile device communication protocol); or any other known and available operating system. Hereinafter, the term "Windows™" includes but is not limited to Windows95™, Windows NT™, Windows98™, Windows CE™ and any upgraded versions of these operating systems by Microsoft Corp. (USA).

Hereinafter, the term "computing platform" refers to any particular operating system and/or hardware device, as previously described, according to which the format for data communication is determined.

Hereinafter, the term "Web browser" refers to any software program which can display text, graphics, or both, from Web pages on World Wide Web sites. Hereinafter, the term "Web page" refers to any document written in a mark-up language including, but not limited to, HTML (hypertext mark-up language) or VRML (virtual reality modeling language), dynamic HTML, XML (extended mark-up language), WML (wireless mark-up language) or related computer languages thereof, as well as to any collection of such documents reachable through one specific Internet address or at one specific World Wide Web site, or any document obtainable through a particular URL (Uniform Resource Locator). Hereinafter, the term "Web site" refers to content

which is provided through a mark-up language or an equivalent thereof. Hereinafter, the term "Web server" refers to a server for providing one or more Web pages to a Web browser upon request.

Hereinafter, the phrase "display a Web page" includes all actions necessary to render at least a portion of the information on the Web page available to the computer user. As such, the phrase includes, but is not limited to, the static visual display of static graphical information, the audible production of audio information, the animated visual display of animation and the visual display of video stream data.

Hereinafter, the term "Web session" is defined as a continuous sequence of HTTP requests and replies, WAP requests and replies, or any other request and reply combination according to a communication protocol between a Web browser and a specific Web site, such that communication between the Web browser and the Web site is performed according to the particular protocol.

Hereinafter, the term "user" refers to an individual who interacts with, or "uses", a Web browser.

Hereinafter, the term "content provider" refers to an entity which makes a wide range of content available through a network, including but not limited to, information, commercial content, video data, and audio data. In addition, the network through which such content is provided could be any of a number of different infrastructures, including but not limited to, WAP (wireless application protocol), SMS (short message system), voice channels and the Internet.

The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware or firmware, or a combination thereof. For the present invention, a software application could be written in substantially any suitable programming language, which could easily be selected by one of ordinary skill in the art. The programming language chosen should be compatible with the computer hardware and operating system according to which the software application is executed. Examples of suitable programming languages include, but are not limited to, C, C++ and Java.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is of a method and a system for protecting the privacy of the user, while enabling the user to predetermine the disclosure of selected items of information to

particular Web sites, for example according to the type of Web site and/or the type of information.

The conceptual model behind the method and system of the present invention involves an extension to Web sessions through the Internet, which allows the content provider to receive at least a portion of the information from the personal profile of the user who initiated the session. The personal profile preferably contains a plurality of items of information which can be used by content providers for tailoring the Web page content to the needs and interests of the user. Optionally, content providers may be interested in only certain items of information in the personal profile, such that only these items are relevant to the tailoring of content from that particular Web site. More preferably, the user is able to add and remove information. and to otherwise modify the personal profile.

This personal profile information is preferably available to the content provider as soon as the Web server for the Web site receives an HTTP or WAP request from the Web browser of the user. Optionally and more preferably, the content provider could then immediately tailor the provided Web page content to the interests of the user, such that the HTTP or WAP reply would contain content which is more closely suited to the user.

However, the personal profile also contains a disclosure policy, which enables the user to control the dissemination of the personal profile information. The disclosure policy preferably determines how, to which Web content provider(s) and under which circumstances the information from the personal profile is disclosed. More preferably, the disclosure policy also includes specific rules for the disclosure of items of personal profile information. Optionally, general rules for the release of items from the personal profile are also included in the disclosure policy.

According to a preferred embodiment of the present invention, the item of information as disclosed may be different than the stored item of information in the user profile. For example, if the age of the user is 27 years, then the age is optionally disclosed as "25-30 years" as a range, rather than as an exact numerical value. The item of information is also optionally disclosed as a range for non-quantitative values, in which the non-quantitative value is characterized according to a text description. For example, if the user enjoys fishing and hiking, then the non-quantitative value disclosed could be "enjoys outdoor activities".

An exemplary disclosure policy is shown in Table 1 below.

Table 1.

Information Type	*Value*	*Disclosure Policy*
Age	28	Ask
Gender	Female	Always
Nutrition Preferences	Vegetarian	www.food. com only
Home Address	21 Main Street, Anytown, USA	Ask
Credit Card Number	1234 5678 1234 5678	Ask

In this example, whenever a content provider requests a certain item of information, such as the gender of the user, which is marked as "Always", the content provider always receives this item of information.

However, if the content provider requests an item which is marked as "Ask", such as the age of the user, then permission is first requested from the user. For example, an explicit confirmation window could be displayed through the GUI (graphical user interface) of the display screen of the user, requesting confirmation for the disclosure of the age of the user. The item of information is then provided to the content provider only if the user confirms that such a disclosure is permitted. Preferably, information which is considered to be particularly sensitive or private, such as the address of the user or the credit card number of the user, is only provided upon receipt of the approval of the user, such that these types of information are preferably marked as "Ask".

Other items of information are optionally automatically provided only to certain Web page providers, such as the nutrition preferences of the user in this example, which are only provided to "www.food.com", but which are always provided to this Web site.

Optionally and more preferably, as described in greater detail below, the user is able to simultaneously determine the behavior of a plurality of information items with a single attribute. Most preferably, this attribute is expressed as a "browsing mode", in which the behavior of the selected information items corresponds to the type of Web browsing session and corresponding Web browser behavior which have been selected by the user. This preferred embodiment enables the user to control the behavior of these information items in a more efficient manner, without the requirement for the user to determine the level of disclosure for each information item individually.

Preferably, the content provider is able to retrieve user information from the personal profile of the user through a personalization API (Application Programming Interface).

According to preferred embodiments of the present invention, the content provider which controls a Web site also creates a content provider profile, of information which the content provider wishes to receive from the user. Preferably, the content provider profile is created from a set of keywords or other disclosure items, from which the content provider may select the most relevant keyword(s) in order to describe the desired information. The same set of keywords is also used to create the personal profile of the user. More preferably, the set of keywords is dynamically created according to requests of the content providers. Optionally and most preferably, the general request of the content provider is performed before information is requested from any specific user.

The request for a particular Web site by a user then more preferably triggers a process of negotiation, in which the content provider profile is compared to the personal profile of the user. If the disclosure policy of the user matches the requested information of the content provider, then the information of the user is disclosed to the content provider. Otherwise, specific questions may optionally be given to the user, in an effort to gather more information, for example, as part of the negotiation process.

According to other preferred embodiments of the present invention, the personal profile of the user is built dynamically, more preferably from a plurality of sources of information. These sources may optionally include, but are not limited to, any one or more of the following sources of information: information disclosed by the user in response to direct interactions with the system of the present invention, for example in response to direct questions from the system of the present invention; information disclosed by the user upon interacting with a Web site which has been registered with the system of the present invention; information disclosed by the user to a Web site which has not been so registered; and information gathered from examining user behavior at a Web site, regardless of whether that Web site is registered with the system of the present invention. However, preferably, only Web sites for content providers which are registered with the system of the present invention would trigger the process of profile matching between the content provider and the user.

The present invention increases the efficiency of interactions between a user and a content provider, while preserving the privacy of the user, by first disclosing only information which is mutually requested by the content provider and by the user for disclosure. Such restricted disclosure both preserves the privacy of the user at a level which is specifically desired by the user. and also prevents the content provider from being flooded with irrelevant information. In addition, the process of negotiating the level of disclosure is automatic, thereby

reducing the level of bandwidth which is required to handle the process of disclosure. At the very worst, the number of required exchanges of information would be the same as without the system of the present invention. However, more typically the system of the present invention would significantly reduce the number of required interactions between the user and the content provider in order to negotiate the process of disclosure, thus increasing the efficiency of interactions between the user and the content provider. This increased efficiency is particularly useful for WAP (Wireless Application Protocol)-enabled devices, such as cellular telephones which receive Web pages for example.

The present invention has the advantage of comprehensively protecting the privacy of the user, by separating various types of information about the user from the identity of the user. If the user does not provide personal identifying information during a session, such as name, address, credit card number, passport or other identification number, and so forth, then the user remains anonymous to the content provider throughout the session. Furthermore, the user has more complete control over the personal data which is stored in the personal profile of the user. Preferably, the user is able to edit or otherwise alter the data upon request. As described in greater detail below, more preferably the data is actually stored on a personal device of the user, such as a cellular telephone for example, which provides even greater control by the user over access to the data in the user profile.

The principles and operation of a system and a method according to the present invention may be better understood with reference to the drawings and the accompanying description, it being understood that these drawings are given for illustrative purposes only and are not meant to be limiting. Although the present invention is described with regard to Web pages, such as HTML (hyper-text mark-up language) and/or WML (wireless mark-up language) documents for example, it is understood that this is for the purposes of discussion only and is without any intention of being limiting. The present invention is also operative with other protocols for transmitting and/or displaying information, including but not limited to, audio (voice) data and SMS (short message system) messages.

Referring now to the drawings, Figure 1 is a flowchart of an exemplary method for determining a personal profile and disclosure policy according to the present invention. In step 1, the user is preferably presented with a template for entering items of information for the personal profile. More preferably, this template includes various types of entries, such as the name and address of the user, which are assumed to be of general interest to users. In step 2, the user enters the type of information into the "Information Type" field, unless this field has

already been filled as part of the template. In step 3, the user enters a value for the information item in the "value" field, which could be the name of the user for a "user name" information element, for example.

In step 4, the user enters a type of disclosure which is permitted for the item of information. As previously described, such a type of disclosure optionally is limited to a single value, such as "Always", if the content provider is to always receive this item of information; or "Ask", if permission must first be requested from the user for providing the item of information to the content provider. Optionally and preferably, such a type of disclosure may have a plurality of values if the item of information is only to be provided to one or more content providers, but is always to be given to these content providers. Also optionally, the type of disclosure may be to disclose a range of values, whether numerical or non-quantifiable, to the content provider.

Alternatively and preferably, the type of disclosure for the information is selected according to one of a plurality of browsing modes. As previously described, such a browsing mode enables the user to simultaneously determine the behavior of a plurality of information items with a single attribute. The user enters the type of disclosure for the item of information which is to be permitted in each browsing mode. The browsing modes are more preferably selected such that a content provider is not able to easily identify the user, unless such identification is desired by the user.

As an illustrative example only, and without any intention of being limiting, most preferably the browsing modes are determined according to the AIDA model (P. Kotler, *Marketing Management*, Prentice Hall International, 1999). In this model, the consumer is assumed to have four behavioral responses: Attention, Interest, Desire and Action, from which the acronym, AIDA, is derived. A browsing mode is optionally and preferably associated with each behavioral response.

In Attention Mode, the purpose of the content provider is to obtain the attention of the user, and then to increase the level of interest of the user. Information disclosed in this browsing mode preferably enables the content provider to determine which content is of interest to the user. The user preferably remains anonymous in this mode, and only reveals general interests and general preferences such as the preferred language of communication, and so forth.

In Interest Mode, the user is performing a search and/or an inquiry for additional information. The user is therefore expected to be generally interested in a type of product or service. For example, the user may be interested in receiving more information about features,

availability, prices and so forth. Preferably, information which is disclosed in this mode, such as age and gender for example, is to reduce the amount of searching which must be performed by the user, and to improve the quality of information which is received by the user. This issue is particularly important for displaying information through WAP, since the small screen and keyboard renders performing a search through a wireless device significantly more difficult.

In Desire Mode, the user indicates interest in a specific product or service. The content provider should offer the best possible solution to the user. In turn, the user may optionally choose to disclose useful information about lifestyle, spending behaviors, expected quality and time constraints. The content provider optionally and preferably provides the user with information about decisions made by other users who share the same lifestyle and/or time constraints, for example, in order to better address the needs of the user. More preferably, the user remains anonymous in this mode.

In Action Mode, the user decides to perform a particular transaction with a particular content provider, or at the very least, indicates an interest in receiving a good or a service from the content provider. Information concerning the identity of the user, such as the user name, credit card information or information concerning other modes of payment, and billing and/or shipping addresses may also optionally be revealed at this stage. Preferably, information which is not directly related to the transaction, such as information concerning the interests of the user for example, is preferably not revealed in this mode, for more rapidly and efficiently conducting the transaction.

For ease of implementation, optionally and preferably each browsing mode is implemented with a different communication channel, such as a socket for example, and hence a different connection to the Web server. Therefore, the Web server would perceive a single Web session as up to four different independent connections, for the above model, or more generally as many different independent connections as the number of different browsing modes which are included in the model.

An example of a completed personal profile with disclosure policy according to the preferred embodiment of the present invention is given in Table 2 below. As shown, the type of permitted disclosure is set for each browsing mode separately.

Table 2.

Information Type	*Value*	*Attention*	*Interest*	*Desire*	*Action*
Age	28	Never	Ask	Always	Never
Gender	Female	Always	Always	Always	Never
Nutrition Preferences	Vegetarian	www.food.com only	www.food.com only	www.food.com only	Never
Home Address	21 Main Street, Anytown, USA	Never	Never	Never	Always
Credit Card Number	1234 5678 1234 5678	Never	Never	Never	Always

Figures 2A and 2B are flowcharts of exemplary methods according to the present invention for handling HTTP cookies. Although these methods are described with regard to HTTP cookies, it is understood that this is for the purposes of illustration only and is without any intention of being limiting, as these methods could also be used with the equivalent data structures of WAP.

As previously described, cookies are currently used for identifying returning visitors to a Web site. Preferably, these cookies are intercepted before being sent from the Web server to the Web browser, in order to prevent the unauthorized disclosure of information. However, HTTP cookies may still be required in certain situations, for example in order to implement certain features such as shopping carts on Web sites. Therefore, the methods described in Figure 2 enable cookies to be used where necessary, while still blocking the unauthorized disclosure of information. Each browsing mode could be associated with one or more methods for handling cookies. According to the present invention two exemplary methods are provided, described in Figures 2A and 2B.

Figure 2A describes a method for handling HTTP cookies by cookie mangling, which is preferred for the first three browsing modes of the preferred embodiment of the present invention (Attention, Interest and Desire). The method is generally suitable for any browsing mode in which the user wishes to remain anonymous, although optionally portions of the personal profile could be disclosed to the content provider.

In step 1, a Web server requests the issuing of an HTTP cookie. In step 2, the request is intercepted by a HTTP proxy server according to the present invention. In step 3, the HTTP proxy server preferably compares the requested HTTP cookie to cookies which have been stored at the proxy server. Preferably, only a single instance of each cookie from each Web server is stored at the proxy server, even if multiple users have visited the Web site and the Web site attempts to issue a cookie for each user.

In step 4, if the proxy server accepts the request for the new cookie, then the cookie is stored at the proxy server. Optionally, the information contained in the cookie is modified before the cookie is stored.

In step 5, when the cookie is to be sent from the Web browser, the stored cookie is retrieved by the proxy server and sent to the Web server. Thus, the same cookie is preferably used for all users when browsing in one of the Attention, Interest or Desire modes, as previously described.

Figure 2B describes a second exemplary method according to the present invention for handling HTTP cookies by cookie caching. This exemplary method is suitable for Web browsing in the Action mode, or for any mode in which full identification of the user is desirable. This method is particularly preferred for mobile devices, in which the cookies cannot be stored on the mobile device itself.

In step 1, a Web server issues an HTTP cookie for a particular user. In step 2, the cookie is intercepted by the HTTP proxy server. In step 3, the cookie is temporarily cached at the proxy server for the duration of the Web session between the Web server and the Web browser of the user.

In step 4, the cached cookie is retrieved by the proxy server and sent to the Web server. Optionally and preferably, in step 5, the cookie is persistently stored at the proxy server before the session ends, in order to be able to provide the cookie on behalf of the user in a future session conducted in Action mode, or for any future session in which the user is to be identified to the Web site content provider.

Figure 3 is a schematic block diagram of an exemplary system according to the present invention, for operation with the previously described methods and features of the present invention. A system **10** features a Web browser **12**, operated by a user computer **14** as shown. User computer **14** is connected to the Internet **16**, which is in turn connected to a content provider **18** for providing Web page content to Web browser **12**.

Internet **16** is also connected to a personalization server **20** according to the present invention. Personalization server **20** preferably enables the personal profile information to be provided to content provider **18**, as previously described. Personalization server **20** includes a user profile manager **22**, for managing the user profile information. Preferably, the user initializes and configures the user profile through user profile manager **22**, for example through Web browser **12**. User profile manager **22** optionally and preferably generates these configuration Web pages which are sent to Web browser **12** for interaction with the user, for example in order to configure the user profile.

The user profile is more preferably divided into a static profile and a dynamic profile. Optionally, the user profile could also be divided into other profiles. The static profile features items of information which either change infrequently over time or else do not change at all. For example, these items of information may optionally include, but are not limited to, name, address, date of birth, gender, profession, hobbies, travel preferences, taste in food, and payment and shipping information and preferences. The dynamic profile features items of information which change more rapidly over time, and which optionally include, but are not limited to, a search for a particular product and current travel plans.

In addition, user profile manager **22** optionally and preferably supports the display of audit trail log information, and other user application tasks, such as logging into personalization server **20**, changing the user password, and so forth.

User profile manager **22** also provides personal profile information to a session manager **24** during a session between Web browser **12** and content provider **18**. Session manager **24** is responsible for controlling and managing these sessions, for example in order to intercept cookies, and to provide certain items of user profile information as requested by content provider **18** and as permitted by the disclosure policy of the user profile. Session manager **24** preferably implements the type of browsing mode for Web browser **12**, as previously described. Optionally and more preferably, Web browser **12** could be in a first browsing mode for a session with a first content provider **18**, and simultaneously in a second browsing mode for a session with a second content provider **18**. These simultaneous sessions and browsing mode designations are also preferably managed by session manager **24**.

Session manager **24** therefore preferably acts as an HTTP or WAP proxy, for monitoring all HTTP or WAP traffic between Web browser **12** and content provider **18**. Also more preferably, session manager **24** closes any session which remains idle for greater than a predetermined period of time.

According to preferred embodiments of the present invention, session manager **24** communicates with content provider **18** through a secure channel, such as SSL (secure socket layer) for example. Content provider **18** preferably must be registered with session manager **24** before any personal profile information can be received by content provider **18**. In addition, the request from content provider **18** must preferably match a particular currently active session between Web browser **12** and content provider **18**.

According to preferred embodiments of the present invention, personalization server **20** is connected to a database **26**. The previously described user profile information, and other information, is preferably stored at database **26**. Also preferably, a plurality of interfaces is provided for connecting personalization server **20** to the other components of system **10**. In particular, preferably an Internet interface **28** connects session manager **24** and user profile manager **22** to Internet **16**. Also preferably, a database interface **30** connects database **26** to user profile manager **22**.

According to preferred embodiments of the present invention, support is also provided by personalization server **20** for communication with a WAP (wireless application protocol)-enabled device **32**, such as a cellular telephone for example. WAP-enabled device **32** receives WML (wireless mark-up language) documents, written in a specially adapted version of HTML, from a WAP gateway **34**, through which communication is performed with personalization server **20**. Preferably, personalization server **20** features a WAP interface **36** for communication with WAP gateway **34**. Thus, personalization server **20** is preferably able to support WAP-enabled devices **32** for operation with the present invention.

Figure 4 is a flowchart of an exemplary method for profile creation for both content providers and users, and for matching these profiles during the process of disclosure of personal information of the user to the content provider.

As shown, in step 1, a shared set of keywords or other disclosure items for creating the profile of the user and of the content provider is created. This set of keywords describes items of data which the content provider wishes to receive from the user. The set of keywords is preferably at least partially dynamically created according to requests for information of the content providers.

In step 2, the content provider which controls a Web site creates a content provider profile, of information which the content provider wishes to receive from the user. Preferably, the content provider profile is created from the previously described set of keywords or other disclosure items, from which the content provider may select the most relevant keyword(s) in

order to describe the desired information. The content provider profile also optionally and more preferably includes general information about the content provider, such as contact information (name, address, telephone number, etc.) for example.

As part of this process, optionally and most preferably the shared set of keywords is matched against the content provider profile parameters, if these parameters are not identical to the shared set of keywords. Such a matching step is optionally performed manually, in order to make certain that the types of information requested by the content provider match the shared set of such types of information.

In addition, in step 3, optionally and more preferably, the parameters/keywords of the content provider profile are grouped into "phases" or marketing segments of interest to the content provider. These marketing segments enable the content provider to immediately identify the interests of the user according to a predefined set of characteristics, based on market research for example.

In step 4, the same set of keywords is also preferably used to create the personal profile of the user. The personal profile of the user is most preferably built dynamically. As previously described, the personal information for the user is more preferably derived from a plurality of sources, the data for which is then matched to the correct data fields, as represented by the set of keywords. These sources may optionally include, but are not limited to, any one or more of the following sources of information: information disclosed by the user in response to direct interactions with the system of the present invention, for example in response to direct questions from the system of the present invention; information disclosed by the user upon interacting with a Web site which has been registered with the system of the present invention; information disclosed by the user to a Web site which has not been so registered; and information gathered from examining user behavior at a Web site, regardless of whether that Web site is registered with the system of the present invention. The personal profile of the user also optionally and more preferably includes general information about the user, such as contact information for example.

In step 5, the user requests a particular Web site of a content provider which is registered with the system of the present invention. In step 6, a process of negotiation is preferably started, in which the content provider profile is compared to the personal profile of the user.

In step 7, if the disclosure policy of the user matches the requested information of the content provider, then the information of the user is disclosed to the content provider.

Otherwise, in step 8, specific questions may optionally be given to the user, in an effort to gather more information, for example, as part of the negotiation process.

In step 9, the behavior of the user is preferably observed as the user interacts with the Web site, regardless of whether the content provider for the Web site has registered with the system of the present invention.

More preferably, in step 10, if the content provider for the Web site has not registered with the system of the present invention, then a shadow profile for the content provider is created by the system of the present invention. The data which is derived from the behavior of the user is then stored according to the shadow profile. The information from the Web site which has not been registered is preferably analyzed in a partially manual procedure, in which fields for entering user information are identified, and the user is prompted to determine if such information should be added to the personal profile of the user.

The information from the shadow profile is optionally and more preferably stored separately in step 11, in order for such information to be made available to competitors which have registered with the system of the present invention.

Figure 5 is a schematic block diagram of a second exemplary but preferred embodiment of the system of the present invention, in which the present invention is implemented for use with WAP. As shown, a system **40** features a user device **42**, which could be a WAP-capable cellular telephone for example. User device **42** is in communication with a WAP gateway **44**. WAP gateway **44** in turn is connected to a proxy server **46** according to the present invention, with an associated user profile database **48** for storing the information in the personal profile of the user. Proxy server **46** is more preferably an HTTP (HyperText Transfer Protocol) server, or Web server, which is connected to the Internet **50**. Internet **50** in turn is connected to a content provider server **52**, which is controlled by the content provider. Content provider server **52** is also optionally and preferably a Web server, such as an HTTP server and/or WTP server for example.

When the user requests a particular Web page through user device **42**, this request is passed through proxy server **46**, which therefore preferably sees all such HTTP requests. More preferably, proxy server **46** receives a signal from user device **42** that the information being requested is of interest to proxy server **46**, by including a command in the link itself for proxy server **46**. For example, the link could optionally be configured as "http://www.example.com/?proxy_server_name=name_of_Web_page", in which

"?proxy_server_name" is a signal to proxy server **46**, and "name_of_Web_page" is the identifier for the Web page being requested through user device **42**.

Proxy server **46** then attempts to perform a process of profile matching, by comparing the personal profile of the user to the profile of the content provider, as previously described in greater detail. Optionally, the process of profile matching begins by first examining the phase to which the user belongs. Once the phase is determined, preferably the parameters of the content provider profile are divided into two groups: mandatory and optional. More preferably, the parameters are assigned a priority according to importance to the content provider for each group. A maximum number of questions which can be sent to the user is also determined.

Proxy server **46** then determines which user information may be freely given to content provider server **52**. Next, proxy server **46** sends questions to user device **42** for the user, up to the maximum number of questions, in order to obtain permission to give additional information to content provider server **52**. More preferably, proxy server **46** first sends questions to the user from the mandatory category, before any questions are sent from the optional category.

According to preferred embodiments of system **40**, proxy server **46** has three components: a WAP gateway plug-in interface **54**, which is adjusted for WAP gateway **44**; a proxy interface **56**; and a proxy process **58**. Proxy interface **56** preferably transfers information from WAP gateway plug-in interface **54** to proxy process **58**, which then more preferably performs the previously described profile matching process.

According to optional but preferred embodiments of the present invention, the profile information for the personal profile of the user could be stored in a distributed computing environment. For example, the user profile information is optionally stored on a device of the user, such as a cellular telephone. Such an implementation would have the advantage of giving the user additional control over access to the data of the user in the personal profile, since the data could only be accessed from the device of the user. Furthermore, the data would only be accessible when the device of the user is "on-line", or connected to a network such as the Internet.

In addition, more preferably the system of the present invention operates in the background of the user computational environment, such that the actions of the user trigger the operation of the present invention in a transparent manner, without the active intervention of the user.

It will be appreciated that the above descriptions are intended only to serve as examples, and that many other embodiments are possible within the spirit and the scope of the present invention.

WHAT IS CLAIMED IS:

1. A method for controlling disclosure of a plurality of items of information to a content provider by a user, the method comprising the steps of:

(a) associating each item of information with a type of disclosure, such that the disclosure of the item of information to the content provider is determined according to said type of disclosure;

(b) examining said type of disclosure to determine if disclosure of the item of information to the content provider is permitted; and

(c) if disclosure is permitted, disclosing the item of information to the content provider.

2. The method of claim 1, wherein step (b) further comprises the step of requesting disclosure of an item of information by the content provider.

3. The method of claim 1, wherein said type of disclosure is such that the item of information is always disclosed to the content provider.

4. The method of claim 1, wherein said type of disclosure is such that step (b) further comprises the step of requesting permission from the user to disclose the item of information.

5. The method of claim 1, wherein said type of disclosure is determined according to a characteristic of the content provider.

6. The method of claim 5, wherein said type of disclosure is disclosing a range of values for the item of information.

7. The method of claim 1, wherein said type of disclosure is a plurality of browsing modes, such that step (a) is performed separately for each item of information for each of said plurality of browsing modes.

8. The method of claim 7, wherein each browsing mode controls disclosure for a plurality of items of information.

9. The method of claim 1, wherein the user interacts with the content provider through a Web browser, and communication between the content provider and said Web browser is performed through a proxy server, such that said proxy server performs steps (b) and (c).

10. The method of claim 9, further comprising the steps of:

(d) issuing a cookie by the content provider;

(e) intercepting said cookie by said proxy server;

(f) comparing said cookie to a plurality of cookies stored at said proxy server; and

(g) if said cookie is unique, storing said cookie at said proxy server, such that said cookie is not associated with an identity of a particular user.

11. The method of claim 10, further comprising the steps of:

(h) retrieving said cookie from said proxy server; and

(i) sending said cookie to the content provider.

12. The method of claim 9, further comprising the steps of:

(d) issuing a cookie by the content provider for a specific user;

(e) intercepting said cookie by said proxy server; and

(f) storing said cookie temporarily in a cache by said proxy server, such that said cookie is associated with said specific user.

13. The method of claim 12, further comprising the steps of:

(g) retrieving said cookie from said cache; and

(h) sending said cookie to the content provider.

14. The method of claim 9, further comprising the steps of:

(d) issuing a cookie by the content provider for a specific user;

(e) intercepting said cookie by said proxy server;

(f) determining a browsing mode for said Web browser by said proxy server; and

(g) if said browsing mode permits transmission of said cookie, passing said cookie from said proxy server to said Web browser.

15. The method of claim 14, further comprising the steps of:

(h) sending said cookie by said Web browser;

(i) intercepting said cookie by said proxy server; and

(j) sending said cookie to the content provider by said proxy server if said browsing mode permits transmission of said cookie.

16. The method of claim 1, wherein step (a) further comprises the steps of:

(i) creating a content provider profile; and

(ii) organizing the plurality of items of information about the user into a user profile; and wherein step (b) further comprises the step of matching said content provider profile to said user profile in order to determine if the items of information should be disclosed to the content provider.

17. The method of claim 16, wherein said user profile is dynamically created from a plurality of sources of user information.

18. The method of claim 17, wherein said plurality of sources of user information are selected from the group consisting of information disclosed by the user in response to a direct question; information disclosed by the user upon interacting with a Web site of the content provider; and information gathered from examining user behavior at a Web site; and a combination thereof.

19. The method of claim 18, wherein at least one source of information is from a Web site of a content provider without said content provider profile, such that the method further comprises the step of:

(d) creating a shadow content provider profile to store said information.

20. The method of claim 19, wherein step (d) further comprises the steps of:

(i) retrieving information from said Web site;

(ii) analyzing said information to create said shadow content provider profile; and

(iii) storing said information about the user from said Web site in said shadow content provider profile.

21. The method of claim 20, wherein step (ii) is performed in a partially manual procedure, said procedure including the step of identifying fields for entering user information.

22. The method of claim 21, wherein the user is prompted to determine if said information is to be added to said user profile in step (iii).

23. The method of claim 22, wherein said content provider profile and said user profile are created from a set of keywords.

24. The method of claim 18, wherein said user profile is dynamically altered in step (b) if an additional value for said user profile is required by the content provider.

25. The method of claim 24, wherein the user is prompted to determine if said information is to be added to said user profile in step (b).

26. The method of claim 16, wherein said content provider profile and said user profile are created from a set of keywords.

27. The method of claim 26, wherein said set of keywords is dynamically created according to a request from a content provider.

28. A system for controlling disclosure of a plurality of items of information by a user, the system comprising:

(a) a Web site content provider for requesting an item of information from the user in a request;

(b) a proxy server for intercepting said request;

(c) a user personal profile for containing the plurality of items of information, including at least one type of disclosure for determining whether said item of information is disclosed to said Web site content provider by said proxy server.

29. The system of claim 28, wherein the disclosure is controlled for a plurality of Web site content providers and for a plurality of users, the system further comprising:

(d) a central computational device for storing said user personal profile for said plurality of users, said central computational device being accessible by said plurality of Web site content providers.

30. The system of claim 29, further comprising:

(d) a user computational device for storing said user personal profile for the user, such that access to said user computational device is controlled by the user.

31. The system of claim 30, wherein said user personal profile is encrypted before being stored, such that only the user is capable of decrypting said user personal profile.

32. A method for controlling disclosure of a plurality of items of information to a content provider by a user, the content provider having an associated Web site, the method comprising the steps of:

(a) associating each item of information with a type of disclosure, such that the disclosure of the item of information to the content provider is determined according to said type of disclosure;

(b) accessing the Web site by the user;

(c) requesting disclosure of an item of information by the content provider;

(d) automatically examining said type of disclosure to determine if disclosure of the item of information to the content provider is permitted; and

(e) if disclosure is permitted, disclosing the item of information to the content provider.

33. The method of claim 32, wherein steps (c)-(e) are performed automatically, without intervention by the user.

34. A method for controlling disclosure of a plurality of items of information to a content provider by a user, the method comprising the steps of:

(a) receiving the plurality of items of information from the user;

(b) associating each item of information with a type of disclosure according to a request of the user, such that the disclosure of the item of information to the content provider is determined according to said type of disclosure;

(c) storing the plurality of items of information in a database; and

(d) accessing said database by the user to alter an item in said database.

35. A method for controlling disclosure of a plurality of items of information to a content provider by a user, the content provider having an associated Web site, the method comprising the steps of:

(a) associating each item of information with a type of disclosure, such that the disclosure of the item of information to the content provider is determined according to said type of disclosure;

(b) requesting disclosure of an item of information by the content provider;

(c) accessing the Web site by the user;

(d) automatically examining said type of disclosure to determine if disclosure of the item of information to the content provider is permitted; and

(e) if disclosure is permitted, disclosing the item of information to the content provider.

36. A system for controlling disclosure of a plurality of items of information by a user, the system comprising:

(a) a Web site content provider for providing a list of at least one item of information for being requested from each user in a request;

(b) a proxy server for intercepting said request; and

(c) a user personal profile for containing the plurality of items of information, including at least one type of disclosure for determining whether said item of information is disclosed to said Web site content provider by said proxy server.

Figure 1

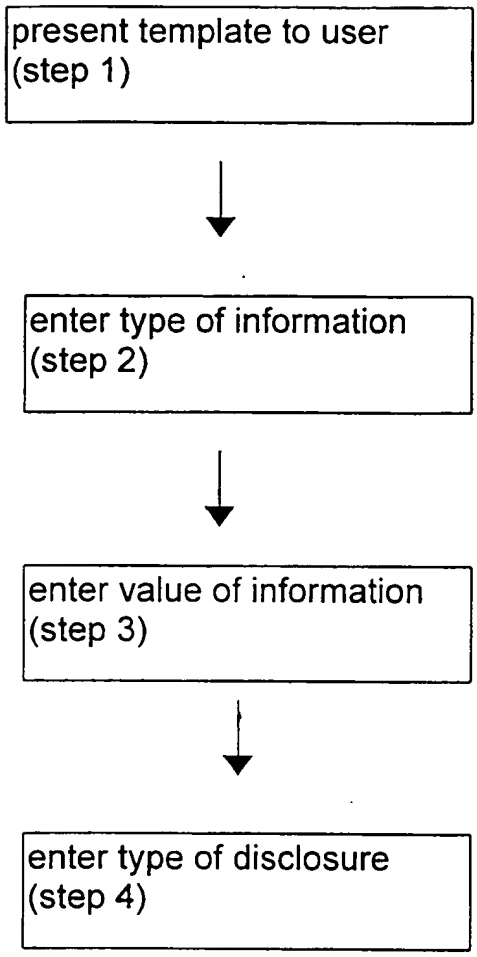

present template to user (step 1)
enter type of information (step 2)
enter value of information (step 3)
enter type of disclosure (step 4)

Figure 2A

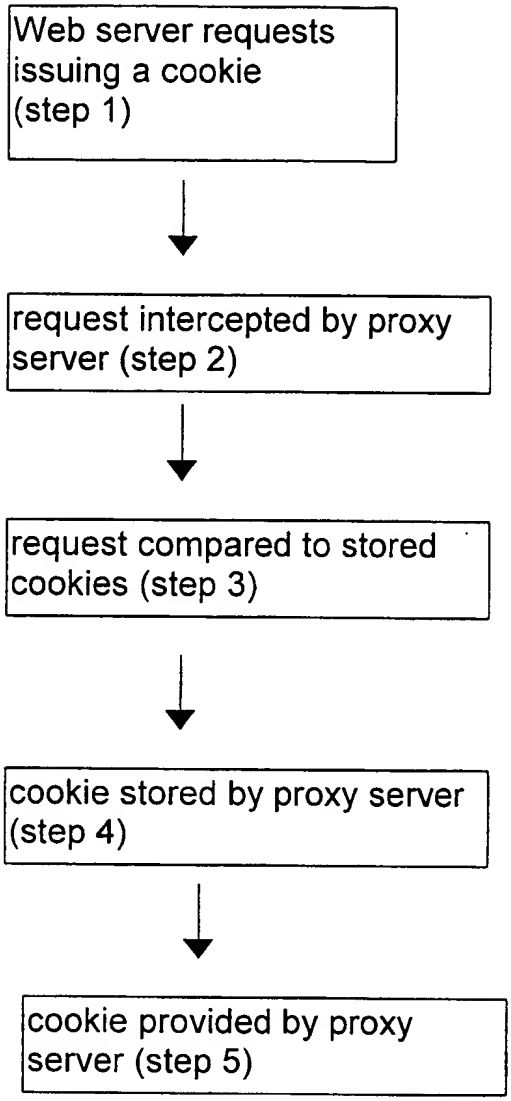
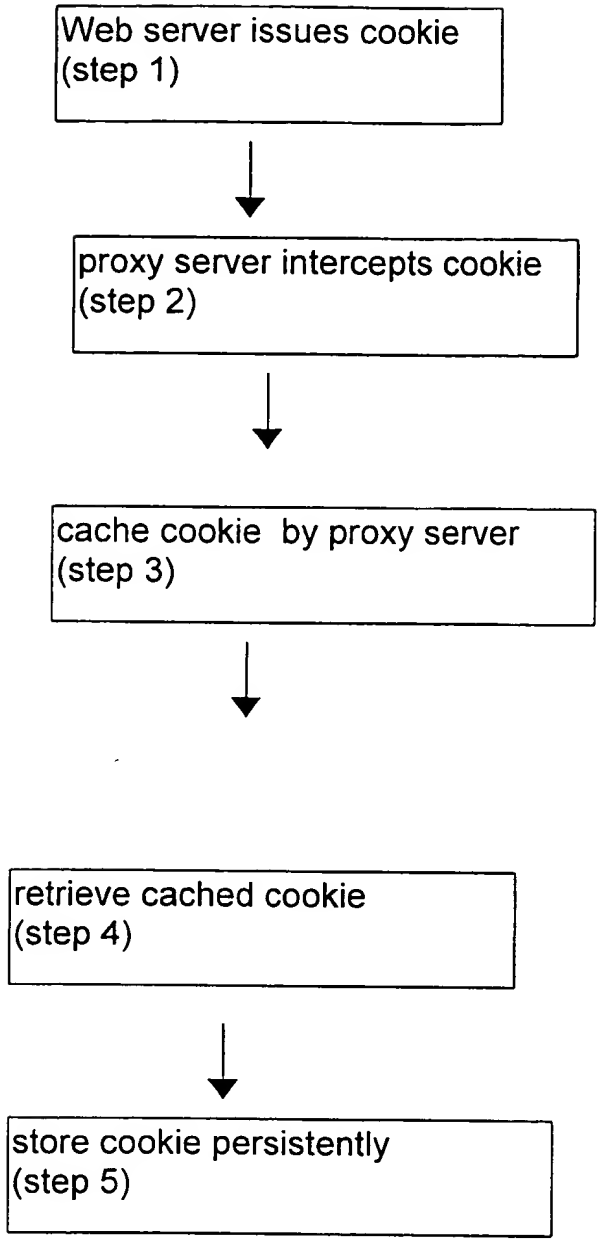

Web server requests issuing a cookie (step 1)
request intercepted by proxy server (step 2)
request compared to stored cookies (step 3)
cookie stored by proxy server (step 4)
cookie provided by proxy server (step 5)

Figure 2B


Web server issues cookie (step 1)
proxy server intercepts cookie (step 2)
cache cookie by proxy server (step 3)
retrieve cached cookie (step 4)
store cookie persistently (step 5)

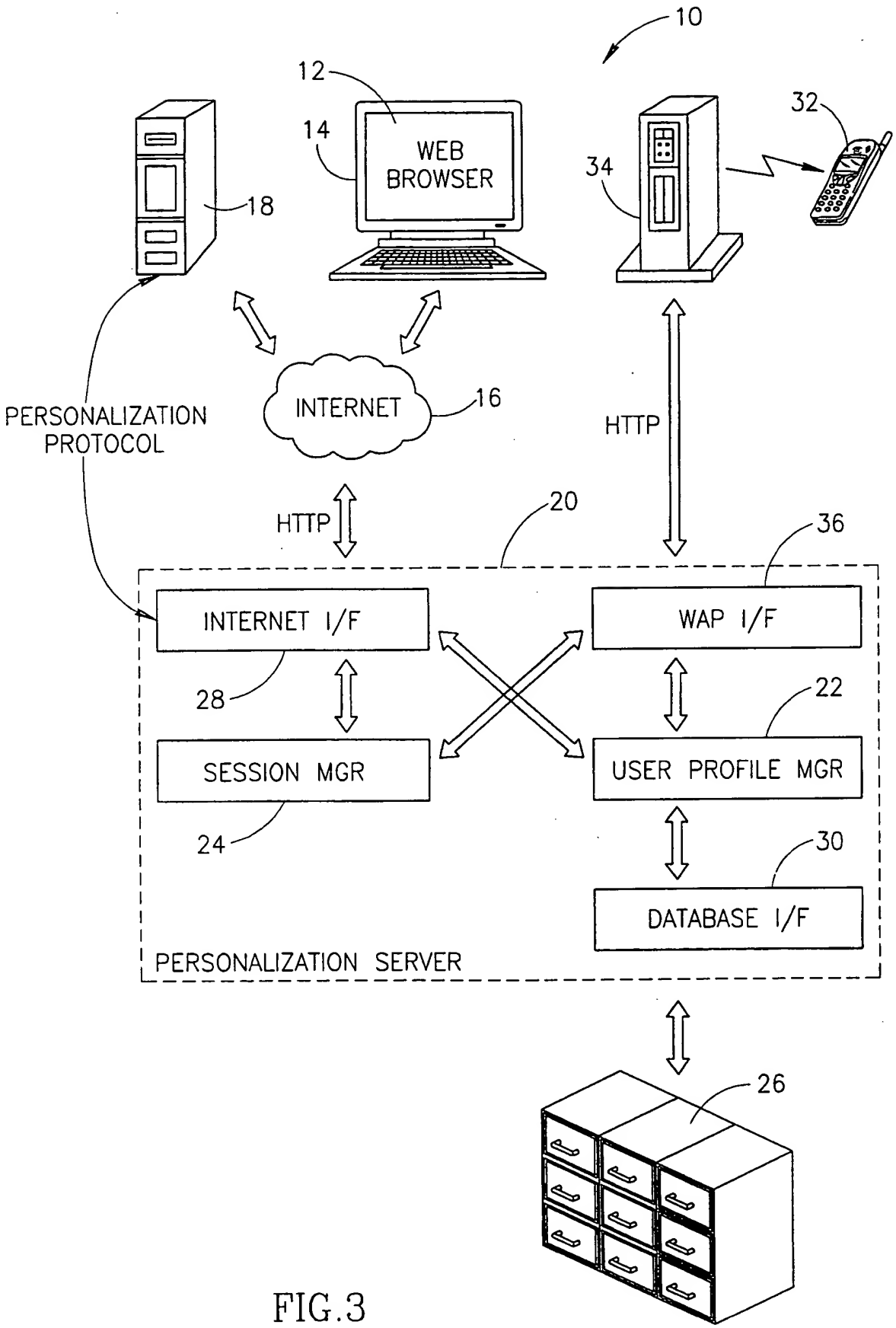

10
12
14
WEB BROWSER
18
32
34
INTERNET
16
PERSONALIZATION PROTOCOL
HTTP
HTTP
20
36
INTERNET I/F
WAP I/F
28
22
SESSION MGR
USER PROFILE MGR
24
30
DATABASE I/F
PERSONALIZATION SERVER
26

FIG.3

Figure 4

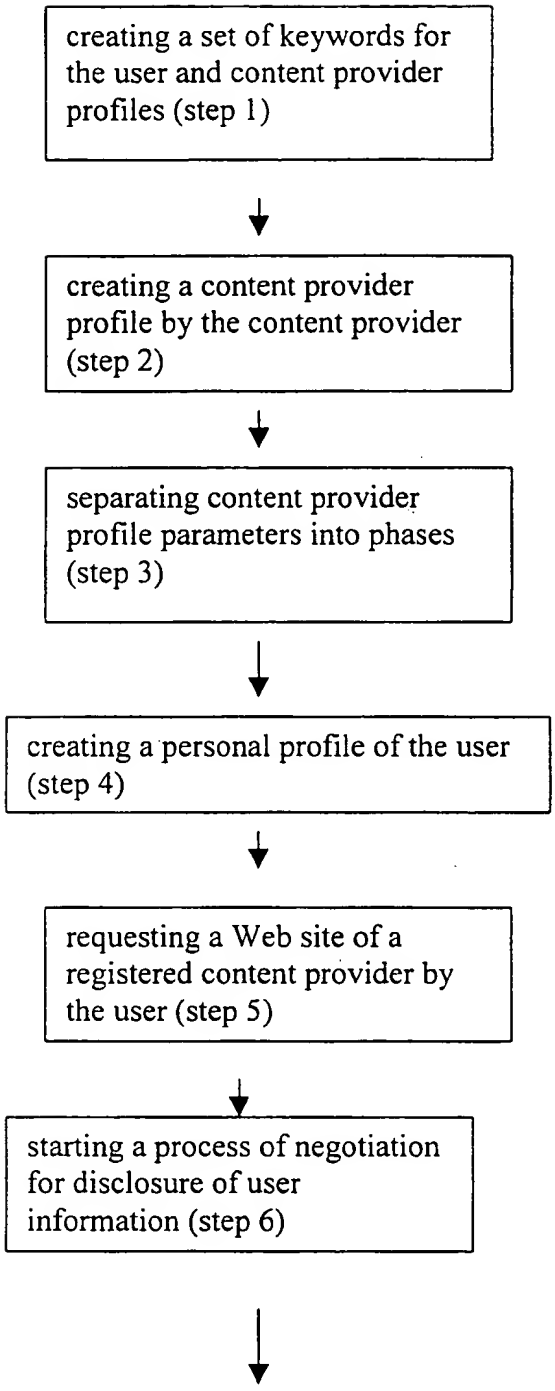

creating a set of keywords for the user and content provider profiles (step 1)
creating a content provider profile by the content provider (step 2)
separating content provider profile parameters into phases (step 3)
creating a personal profile of the user (step 4)
requesting a Web site of a registered content provider by the user (step 5)
starting a process of negotiation for disclosure of user information (step 6)

Figure 4 (con't)

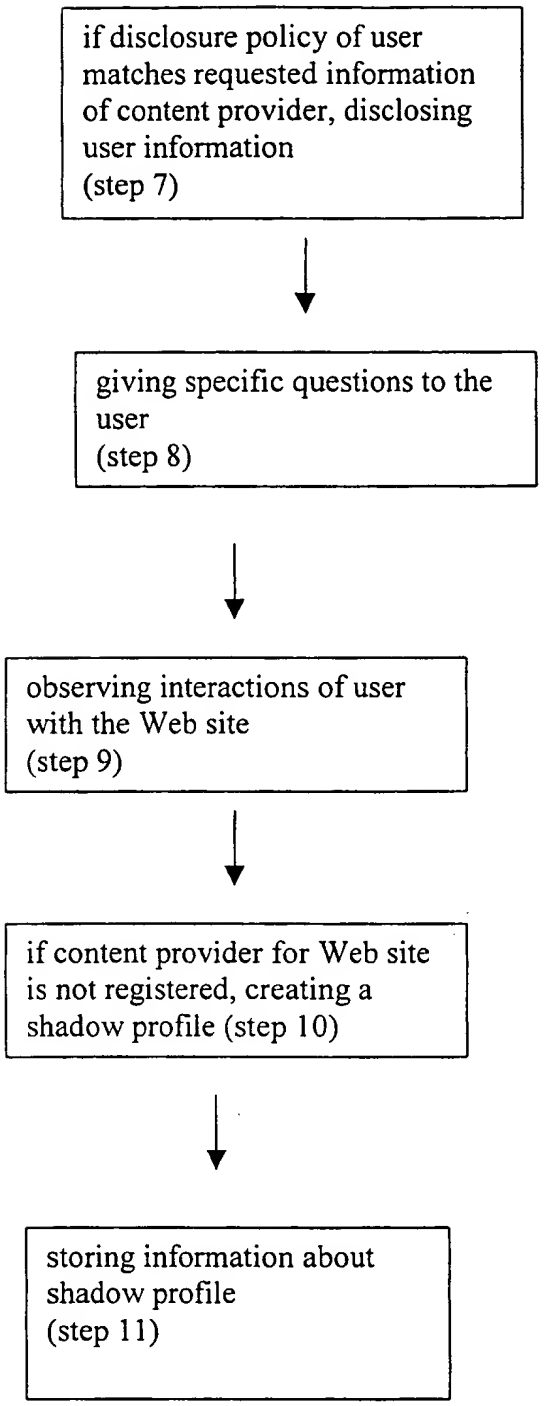
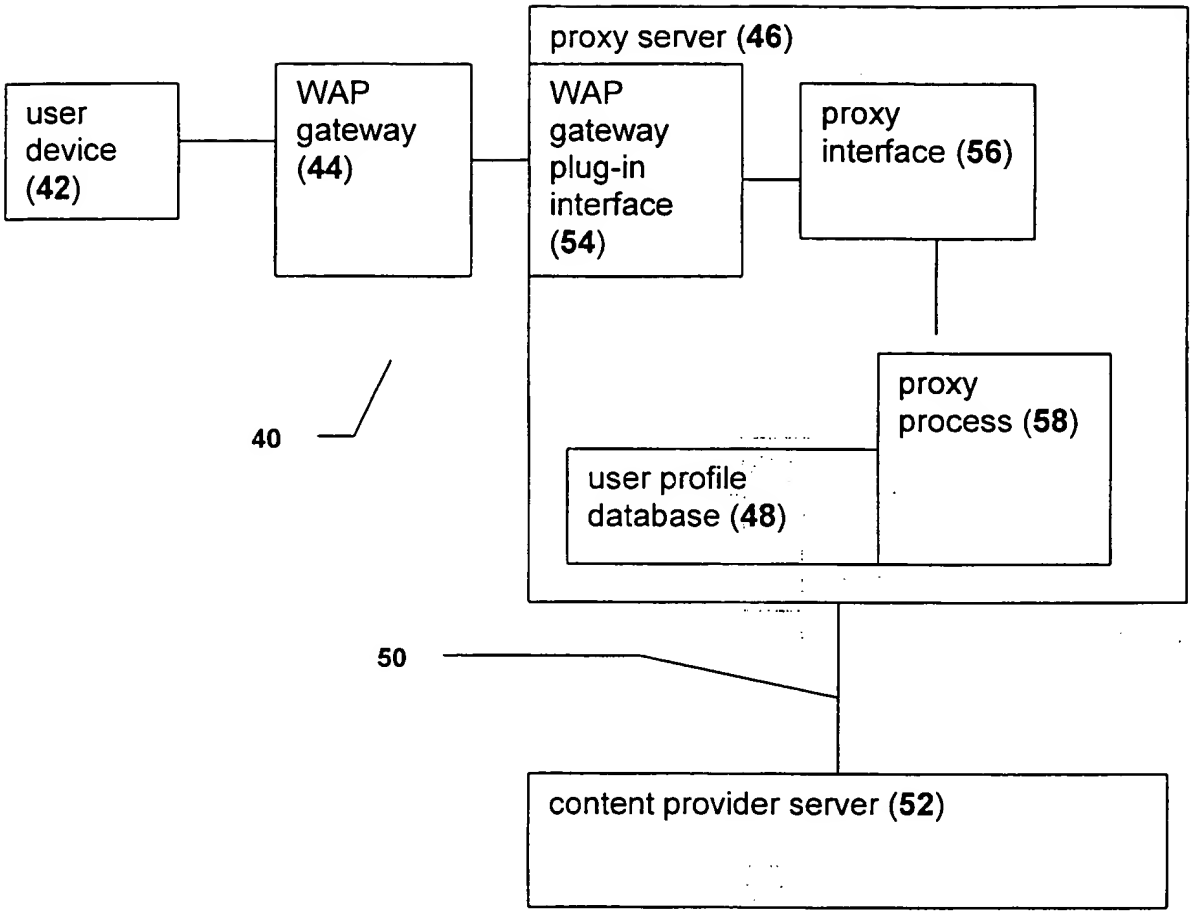


Figure 5


proxy server (46)
user device (42)
WAP gateway (44)
WAP gateway plug-in interface (54)
proxy interface (56)
proxy process (58)
user profile database (48)
40
50
content provider server (52)